REMARKS

In the November 29, 2005 Office Action, claims 1-12, 14-16, 18, and 21-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gentry et al. U.S. Pub No. 20030179885 in view of Goh et al. U.S. Pub. No. 20050102512 and further in view of Forman U.S. Pub. No. 20030120733. Claims 13 and 17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gentry in view of Goh, Forman, and Klos et al. U.S. Pub. No. 20050015449. Claims 19 and 20 were rejected as being unpatentable over Gentry in view of Goh, Forman, and Arcuri et al. U.S. Pub. No. 20040162879. These rejections are respectfully traversed.

Applicants' invention relates to identity-based-encryption (IBE) cryptographic systems. IBE systems may be used to provide secure communications services such as secure email services.

A sender in an IBE system encrypts a message for a recipient using the recipient's IBE public key. The recipient may then decrypt the message using the recipient's corresponding IBE private key. The recipient can obtain the IBE private key from an IBE private key generator associated with the recipient.

Although the sender of the message need not look up the recipient's public key, the sender must obtain IBE public

parameter information that is associated with the recipient's IBE private key generator before the message is encrypted and sent. The IBE public parameter information is used as an ancillary input to the sender's IBE encryption algorithm and works in conjunction with the IBE public key of the recipient to ensure that the message is encrypted properly.

To create the IBE public parameter information and IBE private keys of its associated recipients, an IBE private key generator uses a secret. The security of the encrypted messages associated with this IBE private key generator rests on the ability of the IBE private key generator to maintain the secret confidential. To maintain control over the secret and other aspects of system security, some organizations may want to maintain their own IBE private key generators.

Applicants' invention relates to IBE communications in environments with multiple IBE private key generators. The IBE private key generators and their associated recipients are organized into districts. Each district has a respective IBE private key generator and a number of associated recipients. Each IBE private key generator is responsible for generating IBE private keys for the recipients in its district.

In an environment with multiple IBE private key generators, the operators of the different IBE private key generators may not want to operate their systems identically.

For example, one IBE private key generator may want to authenticate its users with a higher level of authentication than another IBE private key generator. Different IBE private key generators may also want to support different communications protocols or have other customized settings.

With applicants' invention, each district maintains a set of IBE district policy information that describes the policies and protocols for the district. As shown in FIG. 4 of applicants' specification, the IBE district policy information 36 that is associated with district 32 may include IBE encryption protocol information 48, communications protocol information 50, authentication protocol information 52, and content-based protocol information 54. The IBE district policy information 36 is separate from the IBE public parameter information 34 that is used as one of the inputs to the sender's IBE encryption algorithm.

Applicants' claims are directed towards methods for sending IBE-encrypted messages in a system environment in which there are multiple districts. Each district has an IBE private key generator and associated recipients. The sender uses the IBE district policy information associated with a given district in sending messages to recipients in the district. The sender obtains the IBE district policy information from the IBE private key generator in the recipient's district. The IBE district

policy information includes details on the district such as appropriate protocols to be used in sending messages to the recipients in the district. Using the IBE district policy information, the sender can be assured that the IBE message is conveyed properly to the recipient.

Applicants' have amended claim 1 to clarify the type of system environment in which the method of claim 1 applies. Claim 1 has also been amended to make it clear that applicants' method involves using an IBE public key format specified by IBE encryption protocol information to construct an IBE public key for the recipient.

Using the method of amended claim 1, a sender who desires to send a message to a recipient in a given district obtains IBE encryption protocol information over a communications network that specifies which IBE public key format is to be used in constructing IBE public keys for recipients in the given district. The sender then constructs the IBE public key for the recipient according to the specified IBE public key format. In encrypting the message for the recipient, the sender uses (1) the IBE public parameter information associated with the given district (2) the IBE public key of the recipient that was constructed in accordance with the specified IBE public key format.

Nothing like the method of amended claim 1 is shown or suggested in the prior art.

Gentry discloses a hierarchical IBE scheme having a root private key generator (PKG) and multiple lower-level PKGS. In the Office Action (paragraph 4, page 2) it was said that Gentry's "root key generation parameter" constitutes district policy information. Applicants disagree.

The term "root key generation parameter" does not appear in Gentry. Rather, Gentry discloses a "root key generation secret" and "system parameters". The system parameters in Gentry are made public and are an example of IBE public parameter information. The root key generation secret is a sensitive cryptographic secret that is never publicly disclosed. A sender in Gentry's system therefore cannot obtain a copy of a root key generation secret as proposed in the Office Action. Moreover, Gentry's root key generation secret and system parameters do not define any IBE encryption protocols, let alone an IBE public key format.

The Goh patent does not make up for the deficiencies of Gentry. In Goh's system, IBE techniques are used to regulate the printing of documents. As described in paragraph 43 of Goh, printing policies are associated with documents to be printed. A printing policy stipulates requirements for allowing a document to be printed at a printer and is embodied in the IBE

public key Qprint (see, e.g., paragraph 83). As described in paragraph 47, the printing policy may be expressed in any suitable form such as XML format.

Unlike the method defined in claim 1, Goh's sender does not use IBE encryption protocol information specifying an IBE public key format to construct IBE public keys for recipients in a given district. Goh either generates printing policies using a processor 70 that is arranged to allow the generation of a printing policy or receives a printing policy from an external source. (See, e.g., paragraphs 47 and 48 of Goh).

Forman discloses an email system containing a server that maintains a recipient status table and does not make up for the deficiencies of Gentry and Goh.

Claim 1 is therefore allowable over the proposed combination of Gentry, Goh, and Forman. Claims 2-4 and 7-20 are allowable because they depend on claim 1.

New claims 29, 30, and 31 have been added to define further features of applicants' invention.

In view of the foregoing, this application is in

condition for allowance. Reconsideration of this patent application and allowance are respectfully requested.

Respectfully submitted,

G. Victor Treyz 4/18/06

G. Victor Treyz
Reg. No. 36,294
Attorney for Applicants
Customer No. 36532